

Rateless Codes for Finite Message Set

Thesis submitted toward the degree of
“Master of Science in Electrical and Electronic Engineering”

by

Navot Blits

2012

Rateless Codes for Finite Message Set

Thesis submitted toward the degree of
“Master of Science in Electrical and Electronic Engineering”

by

Navot Blits

This research was conducted at the
Department of Electrical Engineering - Systems,

Tel Aviv University

under the supervision of

Prof. Meir Feder

2012

This study was carried out under the supervision of

Prof. Meir Feder

Acknowledgements

I would like to thank my supervisor, Prof. Meir Feder, for his devoted mentoring throughout my research. Without Meir's enthusiasm, curiosity and endless support, this thesis could not have been what it is now. His depth as an information theorist, his broad-mindedness as a scientist and his openheartedness inspired me all along the way. I am grateful for having given the opportunity to walk this path with him.

I would also like to thank Or Ordentlich and Yuval Lomnitz for their interest and insights, which helped me tackle some of the most challenging problems in my research.

Abstract

In this study we consider rateless coding over discrete memoryless channels (DMC) with feedback. Unlike traditional fixed-rate codes, in rateless codes each codeword is infinitely long, and the decoding time depends on the confidence level of the decoder. Using rateless codes along with sequential decoding, and allowing a fixed probability of error at the decoder, we obtain results for several communication scenarios. The results shown here are non-asymptotic, in the sense that the size of the message set is finite.

First we consider the transmission of equiprobable messages using rateless codes over a DMC, where the decoder knows the channel law. We obtain an achievable rate for a fixed error probability and a finite message set. We show that as the message set size grows, the achievable rate approaches the optimum rate for this setting. We then consider the *universal* case, in which the channel law is unknown to the decoder. We introduce a novel decoder that uses a mixture probability assignment instead of the unknown channel law, and obtain an achievable rate for this case.

Finally, we extend the scope for more advanced settings. We use different flavors of the rateless coding scheme for joint source-channel coding, coding with side-information and a combination of the two with universal coding, which yields a communication scheme that does not require any information on the source, the channel, or the amount the side information at the receiver.

Contents

1	Introduction	1
1.1	Background	1
1.2	Thesis Outline	4
2	Definitions and Notation	5
3	Previous Results	9
4	Rateless Coding – Known Channel	13
4.1	Sequential Decoder	13
4.2	Coding Theorem for Known Channel	17
4.3	Error Exponent	19
4.4	Weak Converse	20
4.5	Further Discussions	22
4.5.1	Application for Gaussian Channels	22
4.5.2	Limited Feedback Channel	22
5	Rateless Coding – Unknown Channel	25
5.1	Achievable Rate for an Unknown Channel	25
5.2	Discussion	32
5.2.1	Comparison to the Known Channel Case	32
5.2.2	Induced Error Exponent	33
5.2.3	Training and Channel Estimation	33
6	Extensions	35
6.1	Joint Source-Channel Coding	35

6.2	Source Coding with Side Information	37
6.3	Complete Universality	39
7	Summary	43

List of Figures

Chapter 1

Introduction

1.1 Background

In traditional channel coding schemes the code rate, which is the ratio between the lengths of the encoder's input and output blocks, is an integral part of the code definition. If one of M messages is to be encoded at rate R , then the corresponding codeword has length $n = (\log M)/R$. Provided that the rate is chosen properly, the error probability decreases as M grows. The capacity of the channel C is defined as the largest value of R for which the error probability can vanish.

An alternative approach to fixed-rate channel coding is *rateless codes*. In this approach, we abandon the basic assumption of a fixed coding rate, and allow the codeword length, and hence also the rate, to depend on the channel conditions. When the encoder wants to send a certain message, it starts transmitting symbols from an infinite-length codeword. The decoder receives the symbols that passed through the channel and when it is confident enough about the message, it makes a decision. Perhaps the simplest example of a rateless code is the following (see e.g. [1, Ch.3] or [2, Ch.7]). Suppose that we have a binary erasure channel (BEC) with erasure probability δ . Suppose also that noiseless feedback exists, i.e. the encoder at time instant n has an access to the outputs of the channel at times $1, \dots, n-1$. We use a simple repetition coding, in which each binary symbol is retransmitted until the decoder receives an unerased symbol. Since the erasure probability is δ , the expected number of transmissions until an unerased symbol is

received is $1/(1-\delta)$. This transmission time implies a rate of $1-\delta$, which is exactly the capacity of the binary erasure channel. This simple setting exemplifies some important concepts of rateless codes. First, the transmission time is not fixed, but rather is a random variable (geometrically-distributed in the above case); second, when the length of the transmission is set dynamically, the error probability may be controllable. In this case the transmission is only terminated once the decoder *knows* what message has been transmitted, so the error probability of this coding scheme is zero; third, the code design is rate-independent. In fact, this code can be used for any binary erasure channel; fourth, the continuity of the transmission requires feedback to the encoder. Indeed, as we shall see in this thesis, when rateless codes are used for point-to-point communication, some form of feedback, which can be limited to decision feedback, must exist to enable continuity. However, rateless codes are also invaluable for other settings such as multicast or broadcast communications, in which the existence of feedback is not explicitly required. Shulman [1] introduced the concept of *Static Broadcasting*, in which the transmitter sends a message to multiple users, and each user remains connected until it retrieved enough symbols to make a confident decision. This scheme does not require feedback; the user remains online only as much as it needs, and the rate is determined according to the time the user spent online.

In this thesis we assume a discrete memoryless channel (DMC) with feedback, and devise rateless coding schemes which allow a small (but fixed) error probability ϵ . We investigate the dependence between the rate, the error probability and the size of the message set. The entire analysis is done for a finite message set, and we show that when the size of the message set is taken to infinity, our results agree with classic results from coding theory. We also investigate the rate of convergence to these results. We start by building a simple rateless coding scheme for a known channel. The motivation for this method is due to Wald's analysis (see [3, Ch.3]), where he demonstrated that the Sequential Probability Ratio Test (SPRT) performs like the most powerful test in terms of error probabilities, while using about half the samples on average.

Building on the rateless coding scheme devised for the case of known channel,

we obtain a *universal* channel coding scheme that does not require channel knowledge at the receiver. Unlike previous results on universal decoding, the results here are non-asymptotic and are valid for an arbitrary message set size. We then extend the coding scheme to joint source-channel coding, and show that optimal rate is achievable even when the encoder is uninformed on the source statistics. Next, we use a rateless coding scheme for source coding with side information at the receiver and show that the Slepian-Wolf rate for this scenario is achievable even when the encoder is unaware of the amount of side information. Finally, we show how to combine the above-mentioned techniques with universal source coding, to obtain a scheme that can operate when the statistics of both the source and the channel are unknown, potentially using side information that is obscure to the encoder.

Our work follows previous results discovered by Shulman [1] for the universal case, where the decoder is ignorant of the channel law. In particular, a sequential version of the maximal mutual information (MMI) decoder [4] is used for universal channel decoding and joint-source channel coding, including the case of side information at the decoder. However, the results in [1] are asymptotic in the size of the message set, while the analysis here is made for a fixed size of the message set. For the case of known channel, the decoder used here can be viewed as the counterpart of the sequential MMI decoder that uses the channel law rather than the empirical mutual information. This scheme has been originally introduced by Polyanskiy in [5], where it is proven to achieve the best variable-length coding rate. While the analysis in [5] concentrates on finding the best achievable size of the message set with a constraint on the average decoding time, in this paper we seek the optimum decoding time for a fixed size of the message set. More importantly, the analysis introduced here is then extended naturally to apply for the case of unknown channel, where we use a novel universal decoder, as well as for joint source-channel coding with and without side information at the receiver.

1.2 Thesis Outline

The rest of the thesis is organized as follows. In Chapter 2 we define rateless codes and provide related definitions and notation. In Chapter 3 we survey previous results related to universal communication and rateless codes. In Chapter 4 we treat the case of known channel, for which we obtain an achievable rate using rateless codes. We also prove a converse theorem showing that this rate is asymptotically optimal, and we analyze the rate of convergence. The case of unknown channel is examined in Chapter 5, where we develop a universal decoder and analyze its performance for a general DMC. In Chapter 6 we extend the coding scheme for the case of message sets with non-equiprobable messages, and we also show how rateless coding can be used for problems with side information. Chapter 7 concludes the thesis.

Chapter 2

Definitions and Notation

Throughout this thesis, random variables will be denoted by capital letters and their realizations by the corresponding lowercase letters. Vectors are denoted by superscript that indicate their length, for instance $X^n = [X_1, \dots, X_n]$. Unless otherwise stated, all logarithms are taken to the base of 2. We focus on communication over a discrete memoryless channel (DMC) characterized by a transition probability $p(y|x)$, $x \in \mathcal{X}, y \in \mathcal{Y}$, where \mathcal{X} and \mathcal{Y} are the input and output alphabets of the channel, respectively. With a slight abuse of notation, we use $p(\cdot|\cdot)$ also to denote the joint transition probabilities of the channel, thus $p(y^n|x^n) = \prod_{i=1}^n p(y_i|x_i)$. The capacity of the channel (in bits per channel use) is conventionally defined as $C = \max_{q(x)} I(X; Y)$, where $I(X; Y)$ is the mutual information between the input of the channel and its output, and the maximization is over all channel input priors $q(x)$. If $|\mathcal{X}| = |\mathcal{Y}|$, and $p(y|x) = 1$ if $x = y$ and $p(y|x) = 0$ otherwise, then the channel is said to be noiseless, and in that case $C = \log |\mathcal{X}|$. We also assume that a noiseless feedback exists from the receiver to the transmitter.

A rateless code has the following elements:

1. Message set \mathcal{W} containing M messages. Without the loss of generality we assume that $\mathcal{W} = \{1, \dots, M\}$, with corresponding probabilities $\pi(1), \dots, \pi(M)$. Occasionally, we define $K = \log M$ as the number of bits conveyed in a message.
2. Codebook $\mathcal{C} = \{\mathbf{c}_i\}_{i=1}^M$, where each codeword $\mathbf{c}_i \in \mathcal{X}^\infty$ is generated by

drawing i.i.d. symbols according to a prior $q(x), x \in \mathcal{X}$.

3. Set of encoding functions $f_n : \mathcal{W} \rightarrow \mathcal{X}, n \geq 1$.
4. Set of decoding function $g_n : \mathcal{Y}^n \rightarrow \mathcal{W} \cup \{0\}, n \geq 1$.

Unlike conventional codes, for which the rate is a fundamental property, the above description does not specify a working rate—hence the term *rateless code*. To encode a message $w \in \mathcal{W}$, the encoder starts transmitting the codeword \mathbf{c}_w over the channel. Upon receiving each channel output, the decoder can either decide on one of the messages \hat{w} or decide to wait for further channel outputs, returning ‘0’. Through feedback, the decoder’s decision is known to the encoder, which correspondingly decides whether to transmit further symbols from \mathbf{c}_w or to proceed to the next message. We note that two different forms of feedback can be assumed here: channel feedback and decision feedback. In channel feedback, the encoder at time instance t observes Y^{t-1} , the channel outputs so far, and by imitating the decoder’s operation it becomes aware of any decision made by the decoder. In decision feedback, the encoder is only informed that a decision has been made, and it can proceed to the next message. While channel feedback requires no intervention from the decoder in the feedback process, it essentially assumes that the feedback channel has the same bandwidth as the main channel. Decision feedback, in contrast, requires only one feedback bit per symbol.

We conclude this section with a few definitions required for the next sections.

Definition 1. A *stopping time* T of a rateless code is a random variable defined as

$$T = \min\{n : g_n(Y^n) \neq 0\} \quad (2.1)$$

Definition 2. An *effective rate* R of a rateless code is defined as

$$R = \frac{\log M}{\mathbb{E}\{T\}} \quad (2.2)$$

where $\mathbb{E}\{T\} = \mathbb{E}_q\{\mathbb{E}_p\{T\}\}$, i.e. the averaging is done over all possible codebooks and channel realizations.

Using the definition of stopping time, we can define the error event as the case in which the decoder stops, deciding on the wrong message. The error event conditioned on a particular message is defined as

$$E_w = \{\hat{W} \neq w \mid W = w\} \quad (2.3)$$

where $\hat{W} = g_T(Y^T)$. The average error probability for the entire message set is therefore

$$P_e = \sum_{w=1}^M \pi(w) \cdot \Pr\{E_w\} \quad (2.4)$$

Definition 3. For a given DMC, an (R, M, ϵ) -code is a rateless code with effective rate R , containing M messages and error probability $P_e \leq \epsilon$.

Chapter 3

Previous Results

As noted, the rateless coding scheme is a special case of communication over a channel with feedback. Shannon [6] proved that the capacity of a DMC is not increased by adding feedback. However, adding feedback *can* increase the zero-error capacity of the channel. In his well known paper, Burnashev [7] investigated the effect of feedback in communication over a DMC by analyzing the error exponent of such channel. Introducing the notion of random transmission time, Burnashev obtained a bound on the mean transmission time for a fixed error probability, from which he derived the error exponent¹ for a DMC with feedback. He also proved a converse theorem showing that the expected transmission time, hence also the error exponent, are asymptotically optimal. (That is, they coincide with the results of the converse theorem as the size of the message set grows to infinity.) The main result of [7] is the following theorem.

Theorem (Burnashev [7]). *The optimum error exponent for a DMC with noiseless feedback is*

$$\lim_{M \rightarrow \infty} -\frac{1}{\mathbb{E}\{T\}} \log P_e = C_1 \left(1 - \frac{R}{C}\right), \quad 0 \leq R \leq C \quad (3.1)$$

where T is the transmission time, R is defined in (2.2) and

$$C_1 \triangleq \max_{(x, x') \in \mathcal{X} \times \mathcal{X}} D(p(\cdot|x) || p(\cdot|x')) \quad (3.2)$$

Examining (3.1) we can observe that whenever $R \geq C$, the error exponent

¹Referred to as *reliability function*.

vanishes, which concurs with Shannon's result [6]. Moreover, whenever the channel has at least two inputs that are completely distinguishable from one another, i.e. $p(y|x) > 0$ and $p(y|x') = 0$ for some $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$, it holds that $D(p(\cdot|x)||p(\cdot|x')) \rightarrow \infty$ and hence also $C_1 \rightarrow \infty$ for that channel. Therefore, the error exponent in that case is infinite at *every* rate below the channel capacity, which implies that the zero-error capacity coincides with the channel capacity C .

Also for the case feedback channels, Shulman [1] developed a coding scheme providing reliable communication over an unknown channel, without compromising the rate. Introducing the concept of *static broadcasting*, which is based on random codebook and universal sequential decoder, he demonstrated that it is possible to achieve vanishing error probability at rate that tends to the capacity of the channel as the size of the message set grows indefinitely. Furthermore, Shulman showed that even if the statistics of the information source is unknown to the transmitter, this scheme achieves the optimal decoding length that would have been achieved if the source were compressed by an optimal source-encoder and the channel were known at both ends. More formally, if K information bits of a source S were to be transmitted over an unknown channel W , then the average decoding length satisfies

$$\lim_{K \rightarrow \infty} \frac{\mathbb{E}\{T\}}{K} = \frac{H(S)}{I(P; W)} \quad (3.3)$$

where P is the codebook generation prior and $I(P; W)$ is the mutual information between the input and the output of the channel W when the input is drawn according to distribution P .

Shulman also used the coding scheme for source-encoding of correlated sources. He demonstrated that using static broadcasting, it is possible to achieve the Slepian-Wolf optimal rate region. Combining all into one communication scheme, the achievable decoding length is

$$\lim_{K \rightarrow \infty} \frac{\mathbb{E}\{T\}}{K} = \frac{H(S|Z)}{I(P; W)} \quad (3.4)$$

where Z is the side information at the decoder. Shulman's work has been the main inspiration for this research.

For the case of unknown channel, Tchamkerten and Telatar in [8] used a rateless coding scheme similar to the one defined in Chapter 2, where the stopping condition is that the mutual information between (at least) one of the codewords and the channel output sequence exceeds a certain time-dependent threshold. The authors proved that this scheme can achieve the capacity of a general DMC.² Moreover, they demonstrated that for the class of binary symmetric channel with crossover probabilities $L \in [0, 1/2)$, this coding scheme can achieve Burnashev's exponent at a rate bounded by any fraction of the channel capacity. The latter result is obtained by using a second coding phase, in which the transmitter indicates whether the decoder's decision is correct (an *Ack/Nack* phase). Tchamkerten and Telatar also demonstrated that for the class of Z channels with parameter $L \in [0, 1)$, the achievable rate can be arbitrarily close to the channel capacity, while the error exponent is infinite. The latter result also coincides with Burnashev's exponent (C_1 in (3.1) is infinite in this case), since error-free communication is attainable for the Z channel.

We note that all the above-mentioned results were asymptotic in the size of the message set. Recently, Polyanskiy, Poor and Verdú in [5] introduced non-asymptotic results for communication over DMC with feedback. Through the use of variable-rate coding and sequential decoding they obtained upper and lower bounds for the maximal message set size for fixed bounds on the error probability and mean decoding length. The authors showed that for an error probability constraint $P_e \leq \epsilon$ and mean decoding length constraint $\mathbb{E}\{T\} \leq \ell$, the maximal message set size $M^*(\ell, \epsilon)$ satisfies

$$\frac{\ell C}{1 - \epsilon} - \log \ell + O(1) \leq \log M^*(\ell, \epsilon) \leq \frac{\ell C}{1 - \epsilon} + O(1) \quad (3.5)$$

The setting of [5], as well as the coding scheme, is similar to the one defined later in Chapter 4. However, while in [5] the optimization is on M , for fixed ϵ and ℓ , we fix ϵ and M and find the optimum mean decoding length. The analysis is slightly different, but the results of Chapter 4 comply with [5]. The analysis in

²Since no assumption has been made on the capacity-achieving prior, authors only demonstrated that the rate approaches $I(PQ)$, where P is the codebook generation prior and Q is the transition probability of the channel.

Chapter 4, coming next, lays the ground for the derivation of our novel results for the case of unknown channel.

Chapter 4

Rateless Coding – Known Channel

4.1 Sequential Decoder

We begin by introducing a rateless coding scheme for noisy channels and analyzing its effective rate, under certain constraints on the size of the message set and the error probability. As will be shown in the sequel, the effective rate is closely related to the channel capacity C . More precisely, we will show that under the conventional setting, in which the size message set is taken to infinity, the effective rate coincides with the capacity of the channel.

Consider a discrete memoryless source with a set of M equiprobable messages, i.e. $\pi(i) = 1/M$, $i = 1, \dots, M$. We use a rateless code as defined in Section 2, where each codeword \mathbf{c}_i , $i = 1, \dots, M$ is generated by drawing i.i.d. symbols according to $q(x)$, the capacity-achieving prior of the channel. The source of randomness generating the codewords is shared by the encoder and the decoder, so that the codebook is known at both ends. The decoder uses the following decision rule:

$$g_n(y^n) = \begin{cases} w, & \prod_{k=1}^n p(c_{w,k}|y_k) \geq A \cdot \prod_{k=1}^n q(c_{w,k}) \\ 0, & \text{if no such } w \text{ exists} \end{cases} \quad (4.1)$$

where $\{c_{w,k}\}_{k=1}^\infty$ are the symbols in \mathbf{c}_w . If the threshold crossing condition in (4.1) is satisfied by more than one codeword, we randomly choose one of them and declare an error. We note here that similar decoders have been proposed

by Polyanskiy [5] and Burnashev [7, Ch.3]. The decision rule at (4.1) can be equivalently written as

$$g_n(y^n) = \begin{cases} w, & z_{w,1} + \dots + z_{w,n} \geq a \\ 0, & \text{if no such } w \text{ exists} \end{cases} \quad (4.2)$$

where

$$z_{w,k} = \log \frac{p(c_{w,k}|y_k)}{q(c_{w,k})}, \quad k = 1, \dots, n \quad (4.3)$$

and we define $a = \log A$.

The above-described coding scheme can be summarized as follows. Having selected a message, the encoder starts transmitting an infinite-length random codeword corresponding to that message. The decoder sequentially receives symbols from this codeword that passed through the channel, and at each time instant k calculates $z_{w,k}$ for $w = 1, \dots, M$. It then updates a set of M accumulators, each corresponding to a possible message, and checks whether any of those crossed a prescribed threshold a . If neither of the counters crossed the threshold, ‘0’ is returned and the decoder waits for the next channel output; if exactly one counter crossed the threshold, the decoder makes a decision; and if more than one threshold crossing occurred, an error is declared. In the two latter cases, the encoder proceeds to the next codeword.

For the above-described scheme we have the following theorem.

Theorem 1. *For the decoder in (4.2) with $P_e \leq \epsilon$, the following effective rate is achievable:*

$$R = \frac{C}{1 + \frac{C - \log \epsilon}{\log M}} \quad (4.4)$$

Proof. Since T is a stopping time of the i.i.d. sequence Z_1, Z_2, \dots , Wald’s equation [3] implies

$$\mathbb{E}\{T\} = \frac{\mathbb{E}\{Z_1 + \dots + Z_T\}}{\mathbb{E}\{Z\}}, \quad (4.5)$$

where $\mathbb{E}\{Z\}$ is the expectation of a single sample Z_i . If X_i and Y_i are input and output of the channel, respectively, then by the definition of Z_i we have

$$\mathbb{E}\{Z\} = \mathbb{E}\{Z_i\} = \mathbb{E}\left\{\frac{p(X_i|Y_i)}{q(X_i)}\right\} = C. \quad (4.6)$$

Furthermore, since the stopping condition was not fulfilled time instant $T - 1$ we have

$$Z_1 + \dots + Z_{T-1} < a \quad (4.7)$$

which implies

$$Z_1 + \dots + Z_T < a + Z_T \quad (4.8)$$

Combining (4.5), (4.6) and (4.8) we obtain

$$\mathbb{E}\{T\} < \frac{a + C}{C}. \quad (4.9)$$

We now tune the threshold parameter a to meet the error probability requirement. Suppose that the stopping time of the correct codeword is T_w . An error occurs if a competing codeword $\mathbf{c}_{w'}$, independent of $\{Y_k\}_{k=1}^\infty$, crosses the threshold before \mathbf{c}_w does. Thus,

$$\Pr\{E_w\} = \Pr\left\{\bigcup_{w' \neq w} \bigcup_{t=1}^{T_w} \left\{\frac{\prod_{k=1}^t p(C_{w',k}|Y_k)}{\prod_{k=1}^t q(C_{w',k})} > A\right\}\right\} \quad (4.10)$$

$$\leq (M - 1) \Pr\left\{\bigcup_{t=1}^{T_w} \left\{\frac{\prod_{k=1}^t p(X_k|Y_k)}{\prod_{k=1}^t q(X_k)} > A\right\}\right\} \quad (4.11)$$

$$\leq (M - 1) \Pr\left\{\bigcup_{t=1}^{\infty} \left\{\frac{\prod_{k=1}^t p(X_k|Y_k)}{\prod_{k=1}^t q(X_k)} > A\right\}\right\} \quad (4.12)$$

where (4.11) follows from the union bound for an arbitrary series $\{X_k\}_{k=1}^\infty$ drawn i.i.d. from $q(x)$, independently of $\{Y_k\}_{k=1}^\infty$. Note that the bound in (4.12) represents the probability that a randomly-chosen codeword will exceed the threshold at any time instant. Define a sequence of random variables

$$U_t = \begin{cases} \frac{p(X_t|Y_t)}{q(X_t)}, & \prod_{k=1}^{t-1} U_k \leq A \\ 1, & \text{otherwise} \end{cases} \quad (4.13)$$

If at instant t the threshold at (4.12) is exceeded for the first time, then we have $U_k = p(X_k|Y_k)/q(X_k)$ for $k = 1, \dots, t$ and $U_k = 1$ for all $k > t$. Therefore, it is easy to see that

$$\bigcup_{t=1}^{\infty} \left\{\frac{\prod_{k=1}^t p(X_k|Y_k)}{\prod_{k=1}^t q(X_k)} > A\right\} \Leftrightarrow \prod_{t=1}^{\infty} U_t > A \quad (4.14)$$

We can also see that $\mathbb{E}\{U_t\} = 1$ for *all* t because

$$\mathbb{E}\left\{U_t \mid \prod_{k=1}^{t-1} U_k > A\right\} = 1$$

since $U_t = 1$ deterministically in this case, and

$$\mathbb{E}\left\{U_t \mid \prod_{k=1}^{t-1} U_k \leq A\right\} = \mathbb{E}\left\{\frac{p(X_t|Y_t)}{q(X_t)}\right\} \quad (4.15)$$

$$= \mathbb{E}\left\{\mathbb{E}\left\{\frac{p(X_t|Y_t)}{q(X_t)} \mid Y_t\right\}\right\} \quad (4.16)$$

$$= \mathbb{E}\left\{\sum_{x \in \mathcal{X}} \frac{p(x|Y_t)}{q(x)} \cdot q(x)\right\} \quad (4.17)$$

$$= 1 \quad (4.18)$$

where (4.17) follows since X_t and Y_t are independent. For an arbitrary N we have

$$\mathbb{E}\left\{\prod_{t=1}^N U_t\right\} = \mathbb{E}\left\{\mathbb{E}\left\{\prod_{t=1}^N U_t \mid \prod_{t=1}^{N-1} U_t\right\}\right\} \quad (4.19)$$

$$= \mathbb{E}\{U_N\} \cdot \mathbb{E}\left\{\prod_{t=1}^{N-1} U_t\right\} \quad (4.20)$$

$$= \mathbb{E}\left\{\prod_{t=1}^{N-1} U_t\right\} = \dots = \mathbb{E}\{U_1\} = 1 \quad (4.21)$$

Since the above holds for all N , we also have

$$\mathbb{E}\left\{\prod_{t=1}^{\infty} U_t\right\} = 1 \quad (4.22)$$

Returning to (4.12), we get

$$\Pr\{E_w\} \leq (M-1) \Pr\left\{\bigcup_{t=1}^{\infty} \left\{\frac{\prod_{k=1}^t p(X_k|Y_k)}{\prod_{k=1}^t q(X_k)} > A\right\}\right\} \quad (4.23)$$

$$= (M-1) \Pr\left\{\prod_{t=1}^{\infty} U_t > A\right\} \quad (4.24)$$

$$\leq \frac{M-1}{A} \quad (4.25)$$

where (4.25) follows from (4.22) and Markov's Inequality. Since the above holds for all $w \in \mathcal{W}$, we also have

$$P_e \leq \frac{M-1}{A} \quad (4.26)$$

By choosing $a = \log M - \log \epsilon$, or equivalently $A = M/\epsilon$, we secure that $P_e < \epsilon$. Substituting a into (4.9) and using Definition 2, we obtain (4.4). \square

It is important to note that the encoding operation is independent of the working rate; the encoder needs to know the channel law only to generate the codebook. However, if the channel is known to belong to a family for which the capacity-achieving prior is known (e.g. the uniform prior for symmetric channel), then the optimal rate can be achieved even when the encoder is uninformed on the channel law. Furthermore, from a practical point of view, using the uniform prior instead of the capacity-achieving prior is known to perform relatively well in many cases. For instance, using a uniform prior in a binary channel will lose at most 6% of the capacity (see [1, Ch.5]).

4.2 Coding Theorem for Known Channel

We will now use the coding scheme developed in Section 4.1 to prove the main result for rateless channel coding. For a fixed error probability, we will obtain an achievable rate using rateless codes. Then, we will prove that this rate is within $O(\log \log M / \log M)$ from the optimal rate achievable with this error probability. Before we get to the main theorem, we prove the following lemma, which facilitates some refinement in the achievable rate.

Lemma 1. *Suppose that an (R, M, ϵ) -code exists for a DMC. Then for any $0 < \alpha < 1$, there also exists an (R', M, ϵ') -code for the same channel, where*

$$R' = (1 - \alpha)^{-1} R \quad (4.27)$$

$$\epsilon' = \alpha + \epsilon - \alpha\epsilon \quad (4.28)$$

Proof. To show that the triplet (R', M, ϵ') is achievable, we use the original code with randomized decision-making at the decoder. For each transmitted message,

the decoder either terminates the transmission immediately and declares an error, with probability α , or uses the original decision rule. Denote the stopping time of the original decoder and the modified one by T and T' , respectively. The expected decision time of the modified decoder is

$$\mathbb{E}\{T'\} = (1 - \alpha)\mathbb{E}\{T\}, \quad (4.29)$$

which implies

$$R' = (1 - \alpha)^{-1}R. \quad (4.30)$$

The error event in the modified scheme is a union of two non-mutually-exclusive events: error in the original decoder and the event of early termination. The probability of this union is

$$\epsilon' = \alpha + \epsilon - \alpha\epsilon. \quad (4.31)$$

Finally, we note that the number of messages in the codebook remains unchanged—which completes the proof of the lemma. \square

Theorem 2. *For rateless codes, the following rate is achievable:*

$$R' = \begin{cases} \frac{1-1/\log M}{1+\frac{C+\log \log M}{\log M}} \cdot \frac{C}{1-\epsilon} & \epsilon > 1/\log M \\ \frac{C}{1+\frac{C-\log \epsilon}{\log M}} & \epsilon \leq 1/\log M \end{cases} \quad (4.32)$$

We note that if ϵ is fixed and M is large enough so that $\epsilon > 1/\log M$, the achievable rate has the following asymptotics:

$$R' = \frac{C}{1-\epsilon} \cdot \left(1 - O\left(\frac{\log \log M}{\log M}\right)\right) \quad (4.33)$$

Proof. Theorem 1 implies that the triplet (R, M, δ) is achievable for all $0 < \delta < 1$, where

$$R = \frac{C}{1 + \frac{C-\log \delta}{\log M}} \quad (4.34)$$

By Lemma 1, we can also achieve (R', M, δ') , where

$$R' = \frac{C}{(1 - \alpha) \left(1 + \frac{C-\log \delta}{\log M}\right)} \quad (4.35)$$

$$\delta' = \alpha + \delta - \alpha\delta \quad (4.36)$$

for all $0 < \alpha < 1$. By choosing

$$\alpha = \frac{\epsilon - \delta}{1 - \delta} \quad (4.37)$$

we obtain

$$R' = \frac{1 - \delta}{1 + \frac{C - \log \delta}{\log M}} \cdot \frac{C}{1 - \epsilon} \quad (4.38)$$

$$\delta' = \epsilon \quad (4.39)$$

Since the foregoing analysis holds for all $0 < \delta < \epsilon$, we can choose $\delta = \min\{\epsilon, 1/\log M\}$ to obtain (4.32). \square

Remark 4.1. If $\epsilon \leq 1/\log M$, the choice $\delta = \epsilon$ implies $\alpha = 0$, that is, no randomization at the decoder. This result could be anticipated, since the randomized decoder trades rate for reliability: it obtains a better effective rate with some compromise on the error probability. Hence, whenever the error probability constraint is more important than the working rate – randomization can only worsen matters.

4.3 Error Exponent

Theorem 2 in the previous section provides a relation between the working rate and the allowed error probability. We will now investigate this dependency in the regime of low error probability by developing the error exponent induced by this coding scheme. Assuming that a low error probability is required, randomization at the decoder is inapplicable, so (4.32) can be rewritten as

$$-\frac{R}{\log M} \log \epsilon = C - R - \frac{CR}{\log M} \quad (4.40)$$

Recall that $R = \log M / \mathbb{E}\{T\}$, so

$$-\frac{\log \epsilon}{\mathbb{E}\{T\}} = C - R - \frac{CR}{\log M} \triangleq E(R) \quad (4.41)$$

We can see that the error exponent is a *linear* function of the rate, which is also the case in Burnashev's analysis (3.1) (albeit with a different coefficient). Furthermore, as M grows, the error exponent converges to $C - R$ and the con-

vergence is dominated by a term of order $O(1/\log M)$, or $O(1/K)$. This term can be interpreted as a penalty for using a finite message set.

4.4 Weak Converse

In the previous section we have seen that if we use a codebook with M messages and allow an error probability $P_e \leq \epsilon$, then we can achieve an effective rate with the following asymptotics:

$$R' = \frac{C}{1-\epsilon} \cdot \left(1 - O\left(\frac{\log \log M}{\log M}\right)\right) \quad (4.42)$$

We will now prove that under the above constraints on the message set and the error probability, the best achievable rate has the same asymptotics. In other words, the achievable rate at (4.32) converges to the optimal rate, and the convergence is dominated by a term of order $O(1/\log M)$.

Theorem 3. *Given a decoder with random¹ stopping time T , any rate for which the probability of error does not exceed ϵ satisfies*

$$R' \leq \frac{C}{1-\epsilon} \cdot \left(1 + O\left(\frac{1}{\log M}\right)\right). \quad (4.43)$$

Proof. Define

$$\mu(n) = H(W|Y^n) + nC. \quad (4.44)$$

By [7, Lemma 2]) we have

$$\mathbb{E}\{\mu(n+1)|Y^n\} - \mu(n) = \mathbb{E}\{H(W|Y^{n+1}) - H(W|Y^n)|Y^n\} + C \geq 0 \quad (4.45)$$

which implies that $\mu(n)$ is a submartingale with respect to the process $\{Y_k\}_{k=1}^\infty$. Therefore we have

$$\begin{aligned} \log M = H(W) &= \mu(0) \\ &\leq \mathbb{E}\{\mu(T)\} \\ &= \mathbb{E}\{H(W|Y^T)\} + C \cdot \mathbb{E}\{T\} \end{aligned} \quad (4.46)$$

¹Fixed stopping time is a private case of random stopping time, in which T takes only one value.

Furthermore, by [7, Lemma 1] we have

$$\begin{aligned}\mathbb{E}\{H(W|Y^T)\} &\leq h(P_e) + P_e \cdot \log(M-1) \\ &< 1 + \epsilon \cdot \log M\end{aligned}\tag{4.47}$$

where (4.47) follows from the requirement $P_e \leq \epsilon$, and from an upper bound on the binary entropy function. Combining (4.46) and (4.47) we obtain

$$\log M < 1 + \epsilon \cdot \log M + C \cdot \mathbb{E}\{T\}\tag{4.48}$$

which implies

$$R' = \frac{\log M}{\mathbb{E}\{T\}} < \frac{C}{1-\epsilon} \cdot \left(1 + \frac{1}{C \cdot \mathbb{E}\{T\}}\right)\tag{4.49}$$

Furthermore, from (4.48) we can see that

$$C \cdot \mathbb{E}\{T\} > (1-\epsilon) \cdot \log M - 1\tag{4.50}$$

and therefore (4.49) can be replaced by

$$R' = \frac{\log M}{\mathbb{E}\{T\}} \leq \frac{C}{1-\epsilon} \cdot \left(1 + O\left(\frac{1}{\log M}\right)\right)\tag{4.51}$$

□

Remark 4.2. While (4.32) approaches (4.51) for large M , the upper bound is not tight for a finite M . Note that the converse used here is “weak”, in that it is based on Fano’s inequality, which is known to be loose in many cases. We conjecture that a strong converse can be found, which will be tighter (i.e. closer to (4.32)) even in the non-asymptotic realm.

Remark 4.3. Equation (4.33), the achievable rate, is essentially equivalent to the left-hand side of [5, Eq.18], and equation (4.51), the upper bound on the rate, is equivalent to the right-hand side of that equation. Note, however, that the formulation is slightly different: in [5] size of the message set M is optimized with constraint on the maximal transmission time, while here M is fixed and the transmission time is minimized.

4.5 Further Discussions

4.5.1 Application for Gaussian Channels

While the analysis in Sections 4.1 and 4.2 is done for discrete channels, it can be easily extended to memoryless Gaussian channels. Suppose that X_t and Y_t are the input and output of an additive white Gaussian noise channel at time instant t , i.e.

$$Y_t = X_t + V_t, \quad t = 1, 2, \dots \quad (4.52)$$

where $\{V_t\}_{t=1}^\infty$ is a sequence of i.i.d. Gaussian RV's with zero mean and a known variance. The encoding and the decoding processes, as well as the expression for the resulting effective rate, are similar to those of the DMC, where $q(\cdot)$ is the codebook generation PDF and $p(\cdot|\cdot)$ is the transition PDF of the backward channel.

Specifically, consider the above-described setting where $V_k \sim N(0, \theta)$. Suppose that the codebook is Gaussian with power constraint P , i.e. $C_{m,k} \sim N(0, P)$ for all m, k . (Here again, $C_{m,k}$ is the k -th symbol of the m -th codeword.) The decoding rule is given by (4.1), where

$$p(x|y) = \left(2\pi \frac{\theta P}{\theta + P}\right)^{-1/2} \exp \left\{ -\frac{1}{2 \cdot \frac{\theta P}{\theta + P}} \left(x - \frac{P}{\theta + P} \cdot y \right)^2 \right\} \quad (4.53)$$

$$q(x) = (2\pi P)^{-1/2} \exp \left\{ -\frac{x^2}{2P} \right\} \quad (4.54)$$

The effective rate of the decoder is given in (4.4), where

$$C = \frac{1}{2} \log \left(1 + \frac{P}{\theta} \right) \quad (4.55)$$

4.5.2 Limited Feedback Channel

In the forgoing analysis, we assumed that the feedback channel must be used once per each main channel use. In practice, however, it may be desirable to reduce the amount of data transmitted over the feedback channel. For instance, in the case of broadcasting to multiple users, the upstream channel may have a more stringent bandwidth constraint as it must be accessed by all users. It is

therefore interesting to see how lowering the frequency of the feedback affects the performance of the rateless coding scheme. Suppose that we want to use the feedback channel only once per s received symbols. The maximal number of excess symbols transmitted over the main channel (i.e. the number of symbols transmitted after a decoder without feedback limitation would acknowledge the message) is $s - 1$, which implies an effective rate of

$$R = \frac{C}{1 + \frac{(s-1)C - \log \epsilon}{\log M}} \quad (4.56)$$

From (4.56) we see that limiting the feedback frequency has negligible effect if either $s \ll (-\log \epsilon)/C$ or $s \ll (\log M)/C$. In the former case, the required confidence level is high, and in the latter case the messages are long. That is, in both cases the codewords are long with respect to the capacity of the channel, which implies long transmission time. Therefore, in both cases the excess decoding time is small compared to the entire transmission length, and the effect of the limiting the feedback is negligible.

Chapter 5

Rateless Coding – Unknown Channel

In Chapter 4 we assumed that the communication channel, characterized by $p(y|x)$, is known at the receiver end. Assume now, that the underlying channel is unknown to the receiver. The capacity of the channel is known to be achievable in this scenario using sequential versions of the Maximal Mutual Information (MMI) decoder [1], [8]. However, while these schemes provide reliable communication at rate equal to the channel capacity, they assume that the size of the message set M is infinite. In this chapter we try to answer the question whether universal communication is feasible with a finite message set, and if it is, what rates are achievable? As we shall see shortly, it is possible to achieve reliable communication over an unknown channel even when the message set is finite, and we can also bound the rate degradation due to lack of information about the channel law.

5.1 Achievable Rate for an Unknown Channel

Suppose that we wish to communicate over a DMC with unknown (backward) transition probabilities

$$\theta_{ij} = \Pr\{X = i|Y = j\}, \quad i = 1, \dots, |\mathcal{X}| \quad j = 1, \dots, |\mathcal{Y}| \quad (5.1)$$

We use a coding scheme similar to the one described in Chapter 4 with the following modification. Instead of using the true transition probability $p_{\theta}(x^t|y^t)$,

which is unknown to the decoder, we use a *universal* probability assignment defined as

$$p_U(x^t|y^t) \triangleq \int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^t|y^t) d\boldsymbol{\theta}' \quad (5.2)$$

where

$$\Lambda = \left\{ \boldsymbol{\theta}' \in [0, 1]^{|\mathcal{X}||\mathcal{Y}|} \mid \sum_{i=1}^{|\mathcal{X}|} \theta'_{ij} = 1, \quad j = 1, \dots, |\mathcal{Y}| \right\} \quad (5.3)$$

and the weight function $w(\cdot)$ is chosen to be Jeffreys Prior¹, i.e.

$$w(\boldsymbol{\theta}') = \frac{1}{B \sqrt{\prod_{i,j} \theta'_{ij}}} \quad (5.4)$$

where

$$B = \int_{\Lambda} \frac{d\boldsymbol{\theta}'}{\sqrt{\prod_{i,j} \theta_{ij}}} \quad (5.5)$$

Remark 5.1. While the unknown channel is usually characterized by a set of transition probabilities

$$\tilde{\theta}_{ij} = \Pr\{Y = j|X = i\}, \quad i = 1, \dots, |\mathcal{X}| \quad j = 1, \dots, |\mathcal{Y}|$$

the entire derivation here is done for the *backward* channel parameterization given in (5.1). However, this does not need to bother us since the entire analysis assumes a known input prior $q(x)$, and therefore given $\{\tilde{\theta}_{ij}\}$, the parameters in (5.1) are well-defined. Moreover, the region $\tilde{\Lambda}$, induced by $\{\tilde{\theta}_{ij}\}$ and $q(x)$, is clearly contained in the region Λ . Therefore, if a coding scheme is universal with respect to all possible realizations of the backward channel, it is also universal w.r.t. all possible realizations of the forward channel.

The universal probability assignment implies the following decoding rule, which is the universal counterpart of (4.1):

$$g_n(y^n) = \begin{cases} w, & p_U(\mathbf{c}_w|y^n) \geq A \cdot q(\mathbf{c}_w) \\ 0, & \text{if no such } w \text{ exists} \end{cases} \quad (5.6)$$

In Chapter 4 we used Wald's Identity to bound the expected transmission

¹This is also a special case of Dirichlet Distribution.

time, thereby obtaining an effective rate for the sequential decoder. Unfortunately, in the universal case $p_U(\cdot|\cdot)$ is not necessarily multiplicative, so $\log p_U(\cdot|\cdot)$ cannot be expressed as the sum of i.i.d. random variables. Therefore, the expected transmission time in the universal case cannot be calculated directly by applying Wald's identity. Nevertheless, as we shall see shortly, we can use the results for the known channel case to obtain an upper bound for the transmission time in the universal case.

The following lemma shows that given two sequences x^t and y^t , the universal metric cannot be too far from the conditional probability assignment that is optimally fitted to x^t and y^t .

Lemma 2. *For any two series x^t and y^t we have*

$$\log \frac{p_{\hat{\theta}}(x^t|y^t)}{p_U(x^t|y^t)} \leq \frac{(|\mathcal{X}| - 1)|\mathcal{Y}|}{2} \log \frac{t}{2\pi} + |\mathcal{Y}|\mathcal{K}_{|\mathcal{X}|} + \left(\frac{|\mathcal{X}|^2|\mathcal{Y}|}{4} + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \right) \log e \quad (5.7)$$

where

$$\hat{\theta} = \arg \max_{\theta' \in \Lambda} p_{\theta'}(x^t|y^t) \quad (5.8)$$

and we define

$$\mathcal{K}_{|\mathcal{X}|} = \log \frac{\Gamma(1/2)^{|\mathcal{X}|}}{\Gamma(|\mathcal{X}|/2)} \quad (5.9)$$

Proof. Note that

$$p_{\hat{\theta}}(x^t|y^t) = \max_{\{\theta_{i,j}\}} \prod_{i,j} \theta_{i,j}^{N(x^t,y^t;i,j)} \quad (5.10)$$

$$= \max_{\{\theta_{i,1}\}} \prod_i \theta_{i,1}^{N(x^t,y^t;i,1)} \cdot \max_{\{\theta_{i,2}\}} \prod_i \theta_{i,2}^{N(x^t,y^t;i,2)} \cdot \dots \cdot \max_{\{\theta_{i,|\mathcal{Y}|}\}} \prod_i \theta_{i,|\mathcal{Y}|}^{N(x^t,y^t;i,|\mathcal{Y}|)} \quad (5.11)$$

where

$$N(x^t, y^t; i, j) = |\{k : (x_k, y_k) = (i, j)\}| \quad (5.12)$$

Since both $w(\cdot)$ and $p_{\boldsymbol{\theta}}$ are multiplicative functions, we also have

$$p_U(x^t|y^t) = \int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^t|y^t) d\boldsymbol{\theta}' \quad (5.13)$$

$$= \int_{\tilde{\Lambda}} w(\tilde{\boldsymbol{\theta}}) \prod_i \tilde{\theta}_i^{N(x^t, y^t; i, 1)} d\tilde{\boldsymbol{\theta}} \cdot \int_{\tilde{\Lambda}} w(\tilde{\boldsymbol{\theta}}) \prod_i \tilde{\theta}_i^{N(x^t, y^t; i, 2)} d\tilde{\boldsymbol{\theta}} \cdot \dots \quad (5.14)$$

$$\cdot \int_{\tilde{\Lambda}} w(\tilde{\boldsymbol{\theta}}) \prod_i \tilde{\theta}_i^{N(x^t, y^t; i, |\mathcal{Y}|)} d\tilde{\boldsymbol{\theta}} \quad (5.15)$$

where

$$\tilde{\Lambda} = \left\{ \tilde{\boldsymbol{\theta}} \in [0, 1]^{|\mathcal{X}|} \mid \sum_{i=1}^{|\mathcal{X}|} \tilde{\theta}_i = 1, \right\} \quad (5.16)$$

From [9, Lemma 1] we know that

$$\log \frac{\max_{\{\theta_{i,j}\}} \prod_i \theta_{i,j}^{N(x^t, y^t; i, j)}}{\int_{\tilde{\Lambda}} w(\tilde{\boldsymbol{\theta}}) \prod_i \tilde{\theta}_{i,j}^{N(x^t, y^t; i, j)} d\tilde{\boldsymbol{\theta}}} \leq \frac{|\mathcal{X}| - 1}{2} \log \frac{t}{2\pi} + \mathcal{K}_{|\mathcal{X}|} + \left(\frac{|\mathcal{X}|^2}{4} + \frac{|\mathcal{X}|}{2} \right) \log e \quad (5.17)$$

for all $j = 1, \dots, |\mathcal{Y}|$. Thus, we obtain

$$\log \frac{p_{\hat{\boldsymbol{\theta}}}(x^t|y^t)}{p_U(x^t|y^t)} = \log \prod_j \frac{\max_{\{\theta_{i,j}\}} \prod_i \theta_{i,j}^{N(x^t, y^t; i, j)}}{\int_{\tilde{\Lambda}} w(\tilde{\boldsymbol{\theta}}) \prod_i \tilde{\theta}_{i,j}^{N(x^t, y^t; i, j)} d\tilde{\boldsymbol{\theta}}} \quad (5.18)$$

$$\leq \frac{(|\mathcal{X}| - 1) |\mathcal{Y}|}{2} \log \frac{t}{2\pi} + |\mathcal{Y}| \mathcal{K}_{|\mathcal{X}|} + \left(\frac{|\mathcal{X}|^2 |\mathcal{Y}|}{4} + \frac{|\mathcal{X}| |\mathcal{Y}|}{2} \right) \log e \quad (5.19)$$

$$= \frac{(|\mathcal{X}| - 1) |\mathcal{Y}|}{2} \log t + \beta \quad (5.20)$$

where we define

$$\beta \triangleq |\mathcal{Y}| \mathcal{K}_{|\mathcal{X}|} + \left(\frac{|\mathcal{X}|^2 |\mathcal{Y}|}{4} + \frac{|\mathcal{X}| |\mathcal{Y}|}{2} \right) \log e - \frac{(|\mathcal{X}| - 1) |\mathcal{Y}|}{2} \log(2\pi) \quad (5.21)$$

□

We are now ready to prove the main theorem for rateless coding over an unknown channel.

Theorem 4. *For the decoder in 5.6 with $P_e \leq \epsilon$, the following effective rate is*

achievable:

$$R = \frac{C \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{\log M \ln 2}\right)}{1 + \frac{C + \beta - \log \epsilon + \frac{|\mathcal{X}||\mathcal{Y}|}{2} (\log \log M - \log C - \frac{1}{\ln 2})}{\log M}} \quad (5.22)$$

Proof. The stopping time in the above-described scheme is

$$T = \min \left\{ t : \frac{p_U(x^t|y^t)}{\prod_{k=1}^t q(x_k)} > A \right\} \quad (5.23)$$

since

$$\log p_U(x^t|y^t) = \log p_{\theta}(x^t|y^t) - \log \frac{p_{\theta}(x^t|y^t)}{p_U(x^t|y^t)} \quad (5.24)$$

we have

$$T = \min \left\{ t : \frac{p_U(x^t|y^t)}{\prod_{k=1}^t q(x_k)} > A \right\} \quad (5.25)$$

$$= \min \left\{ t : \log \frac{\prod_{k=1}^t p_{\theta}(x_k|y_k)}{\prod_{k=1}^t q(x_k)} > \log A + \log \frac{p_{\theta}(x^t|y^t)}{p_U(x^t|y^t)} \right\} \quad (5.26)$$

$$\leq \min \left\{ t : \log \frac{\prod_{k=1}^t p_{\theta}(x_k|y_k)}{\prod_{k=1}^t q(x_k)} > \log A + \log \frac{p_{\hat{\theta}}(x^t|y^t)}{p_U(x^t|y^t)} \right\} \quad (5.27)$$

$$< \min \left\{ t : \sum_{k=1}^t \log \frac{p_{\theta}(x_k|y_k)}{q(x_k)} > \log A + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \log t + \beta \right\} \quad (5.28)$$

where (5.27) follows since $p_{\hat{\theta}}(x_k|y_k) \geq p_{\theta}(x_k|y_k)$ by definition (5.8) and (5.28) follows from Lemma 2.

From the same considerations as in the proof of Theorem 1, at the stopping time T we necessarily have

$$\sum_{k=1}^T \log \frac{p_{\theta}(X_k|Y_k)}{q(X_k)} \leq a + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \log T + \beta + \log \frac{p_{\theta}(X_T|Y_T)}{q(X_T)} \quad (5.29)$$

where we define $a = \log A$. By (5.29) and Wald's Identity,

$$\mathbb{E}\{T\} = \frac{\mathbb{E} \left\{ \sum_{k=1}^T \log \frac{p_{\theta}(X_k|Y_k)}{q(X_k)} \right\}}{\mathbb{E} \left\{ \log \frac{p_{\theta}(X|Y)}{q(X)} \right\}} \quad (5.30)$$

$$\leq \frac{a + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \cdot \mathbb{E}\{\log T\} + \beta + C}{C} \quad (5.31)$$

Since $\log_2 u \leq \frac{u}{v \ln 2} + \log_2 v - \frac{1}{\ln 2}$ for all $u, v > 0$, (5.31) implies

$$\mathbb{E}\{T\} \leq \frac{a + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \left(\log v - \frac{1}{\ln 2} \right) + \beta + C}{C \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{C \cdot v \ln 2} \right)} \quad (5.32)$$

For $v = \frac{\log M}{C}$ we obtain

$$\mathbb{E}\{T\} \leq \frac{a + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \left(\log \log M - \log C - \frac{1}{\ln 2} \right) + \beta + C}{C \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{\log M \ln 2} \right)} \quad (5.33)$$

which corresponds to the following effective rate:

$$R = \frac{C \log M \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{\log M \ln 2} \right)}{a + \frac{|\mathcal{X}||\mathcal{Y}|}{2} \left(\log \log M - \log C - \frac{1}{\ln 2} \right) + \beta + C} \quad (5.34)$$

Similarly to the derivation in Chapter 4, we bound the error probability by

$$\Pr\{E_w\} \leq (M-1) \Pr \left\{ \bigcup_{t=1}^{\infty} \left\{ \frac{p_U(X^t|Y^t)}{q(X^t)} > A \right\} \right\}$$

where $\{X_k\}_{k=1}^{\infty}$ and $\{Y_k\}_{k=1}^{\infty}$ are independent sequences. Define

$$\Phi_t = \begin{cases} \frac{p_U(X^t|Y^t)}{p_U(X^{t-1}|Y^{t-1}) \cdot q(X^t)}, & \prod_{k=1}^{t-1} \Phi_k \leq A \\ 1, & \text{otherwise} \end{cases} \quad (5.35)$$

We can see that

$$\bigcup_{t=1}^{\infty} \left\{ \frac{p_U(X^t|Y^t)}{q(X^t)} > A \right\} \Leftrightarrow \prod_{t=1}^{\infty} \Phi_t > A \quad (5.36)$$

Furthermore, we can see that $\mathbb{E}\{\Phi_t\} = 1$ for all t since

$$\mathbb{E} \left\{ \Phi_t \mid \prod_{k=1}^{t-1} \Phi_k > A \right\} = 1$$

and

$$\mathbb{E} \left\{ \Phi_t \middle| \prod_{k=1}^{t-1} \Phi_k \leq A \right\} = \mathbb{E} \left\{ \frac{p_U(X^t|Y^t)}{p_U(X^{t-1}|Y^{t-1}) \cdot q(X_t)} \right\} \quad (5.37)$$

$$= \mathbb{E} \left\{ \mathbb{E} \left\{ \frac{p_U(X^t|Y^t)}{p_U(X^{t-1}|Y^{t-1}) \cdot q(X_t)} \middle| X^{t-1}, Y^t \right\} \right\} \quad (5.38)$$

$$= \mathbb{E} \left\{ \frac{\mathbb{E} \left\{ \int_{\Lambda} w(\boldsymbol{\theta}') \frac{p_{\boldsymbol{\theta}'}(x^t|y^t)}{q(x_t)} d\boldsymbol{\theta}' \middle| X^{t-1}, Y^t \right\}}{\int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^{t-1}|y^{t-1}) d\boldsymbol{\theta}'} \right\} \quad (5.39)$$

$$= \mathbb{E} \left\{ \frac{\sum_{x_t \in \mathcal{X}} q(x_t) \int_{\Lambda} w(\boldsymbol{\theta}') \frac{p_{\boldsymbol{\theta}'}(x^t|y^t)}{q(x_t)} d\boldsymbol{\theta}'}{\int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^{t-1}|y^{t-1}) d\boldsymbol{\theta}'} \right\} \quad (5.40)$$

$$= \mathbb{E} \left\{ \frac{\int_{\Lambda} w(\boldsymbol{\theta}') \sum_{x_t \in \mathcal{X}} p_{\boldsymbol{\theta}'}(x^t|y^t) d\boldsymbol{\theta}'}{\int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^{t-1}|y^{t-1}) d\boldsymbol{\theta}'} \right\} \quad (5.41)$$

$$= \mathbb{E} \left\{ \frac{\int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^{t-1}|y^{t-1}) d\boldsymbol{\theta}'}{\int_{\Lambda} w(\boldsymbol{\theta}') p_{\boldsymbol{\theta}'}(x^{t-1}|y^{t-1}) d\boldsymbol{\theta}'} \right\} = 1 \quad (5.42)$$

For an arbitrary N we have

$$\mathbb{E} \left\{ \prod_{t=1}^N \Phi_t \right\} = \mathbb{E} \left\{ \mathbb{E} \left\{ \prod_{t=1}^N \Phi_t \middle| \prod_{t=1}^{N-1} \Phi_t \right\} \right\} \quad (5.43)$$

$$= \mathbb{E} \{ \Phi_N \} \cdot \mathbb{E} \left\{ \prod_{t=1}^{N-1} \Phi_t \right\} \quad (5.44)$$

$$= \mathbb{E} \left\{ \prod_{t=1}^{N-1} \Phi_t \right\} = \dots = 1 \quad (5.45)$$

Since the above holds for all N , we also have

$$\mathbb{E} \left\{ \prod_{t=1}^{\infty} \Phi_t \right\} = 1 \quad (5.46)$$

Thus, similarly to the case of known channel, the error probability can be bounded by

$$\Pr\{E_w\} \leq (M-1) \Pr \left\{ \bigcup_{t=1}^{\infty} \left\{ \frac{p_U(X^t|Y^t)}{q(X^t)} > A \right\} \right\} \quad (5.47)$$

$$= (M-1) \Pr \left\{ \prod_{t=1}^{\infty} \Phi_t > A \right\} \leq \frac{M-1}{A} \quad (5.48)$$

Here again, we choose $A = M/\epsilon$ to obtain $P_e < \epsilon$. Substituting $a = \log A = \log M - \log \epsilon$ into (5.34) we finally get (5.22). \square

Remark 5.2. Interestingly, the upper bound on the error probability in (4.23), obtained when the decoder uses the known channel law $p(x|y)$, applies for an arbitrary probability assignment $p_U(x|y)$, where the only required constraint is that the latter integrates to unity.

Remark 5.3. As in the case of known channel, we can use randomized decoder here to obtain the following rate:

$$R = \frac{C \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{\log M \ln 2}\right)}{1 + \frac{C + \beta - \log \delta + \frac{|\mathcal{X}||\mathcal{Y}|}{2} (\log \log M - \log C - \frac{1}{\ln 2})}{\log M}} \cdot \frac{1 - \delta}{1 - \epsilon} \quad (5.49)$$

for all $0 < \delta < \epsilon$. As we mentioned in Section 4.2, if the required error probability is small, randomization should not be applied. However, if the error probability constraint is loose enough, a better rate may be obtained by optimizing delta in (5.49).

5.2 Discussion

5.2.1 Comparison to the Known Channel Case

Having obtained achievable rates for the cases of both known and unknown channels, it is interesting to compare these results and evaluate the rate degradation due to the unknown channel. For the case of a known channel, the effective rate at (4.4) can be approximated by

$$R \approx C \left(1 - \frac{C - \log \epsilon}{\log M}\right) \quad (5.50)$$

For the case of unknown channel, we can approximate (5.22) by

$$\begin{aligned} R_U \approx & C \left(1 - \frac{C - \log \epsilon}{\log M}\right) \\ & - C \left(\frac{|\mathcal{X}||\mathcal{Y}|}{2} \frac{\log \log M}{\log M} + \frac{(|\mathcal{X}||\mathcal{Y}|/2 - 1)/\ln 2 + \beta + \log C}{\log M} \right) + O\left(\frac{1}{\log^2 M}\right) \end{aligned} \quad (5.51)$$

Hence, the penalty for lack of channel knowledge amounts to

$$R - R_U = C \left(\frac{|\mathcal{X}||\mathcal{Y}| \log \log M}{2 \log M} + \frac{(|\mathcal{X}||\mathcal{Y}|/2 - 1)/\ln 2 + \beta + \log C}{\log M} \right) + O\left(\frac{1}{\log^2 M}\right) \quad (5.52)$$

The leading term in the latter expression behaves as $O(\log \log M / \log M) = O(\log K / K)$, factorized by the product of the cardinalities of input and output of the channel. It is interesting to compare this result with known results from universal source coding, where the *redundancy*² is dominated by the cardinality of the alphabet of the source [10], and a term that behaves as $O(\log n / n)$, where n is the source length.

5.2.2 Induced Error Exponent

Let us now examine Theorem 4 in light of the previous results. Equation (5.22) implies the following error exponent:

$$-\frac{\log \epsilon}{\mathbb{E}\{T\}} = C - R - \frac{|\mathcal{X}||\mathcal{Y}|}{2} \cdot \frac{\log \log M}{\log M} + O\left(\frac{1}{\log M}\right) \quad (5.53)$$

As in the case of a known channel, we see that the error exponent is a linear function of the rate, but an additional term of order $O(\log \log M / \log M)$ is added. Here again, we interpret this term as a penalty for the lack of channel knowledge at the receiver. Furthermore, by taking $M \rightarrow \infty$, we can also see that (5.53) coincides with [8, Proposition 1].

5.2.3 Training and Channel Estimation

In many practical applications, communication over an unknown channel is done by means of channel estimation. In this approach, the transmission includes predefined *training* signals, which are known to the receiver and are used to estimate the channel parameters. As an alternative to the universal communication scheme introduced in this chapter, we can use the following method. Prior to any message transmission, the transmitter sends a training sequence, which the

²The excess of the average codeword length above the entropy of the source.

receiver uses to estimate the channel. After the training phase, the transmitter sends the message. The receiver uses the *estimated* channel parameters to decode the message, using, for instance, the decoding rule at (4.2). A drawback from this approach is that even after the channel estimation phase, the residual error in the estimated channel parameters will degrade the performance of the decoder. Furthermore, enhancement of the channel estimation accuracy requires long training sequences, which will introduce non-negligible overhead to the transmission time. Clearly, using training will not lead to the convergence rate of (5.52).

Chapter 6

Extensions

6.1 Joint Source-Channel Coding

In the previous chapters we assumed that the messages conveyed over the channel were equiprobable, which is the case if, for instance, the source of information has been compressed and the message W is the output of the source encoder. Assume now, that the messages have arbitrary probabilities $\pi(1), \dots, \pi(M)$. Each message now contains a different amount of information, which would translate into different codeword length at the output of the source encoder. However, in rateless codes the codeword assigned to each message is always infinite, and the actual codeword length is determined by the decoder. (The effective length of the message depends on the decoder's stopping time.) It is therefore tempting to use rateless codes for an uncompressed source and try to achieve good compression rate and reliable communication simultaneously. To simplify matters, we begin by tackling the case of known channel and postpone the analysis for unknown channel to Section 6.3. We use the following generalized version of the encoder (4.2).

$$g_n(y^n) = \begin{cases} w, & z_{w,1} + \dots + z_{w,n} \geq a_w \\ 0, & \text{if no such } w \text{ exists} \end{cases} \quad (6.1)$$

where a_w is a threshold that depends on the message w , and we define $a_w = \log A_w$. Repeating the derivation for the error probability done in the previous

section, we get by Markov's inequality

$$\Pr\{E_w\} \leq \sum_{w' \neq w} \frac{1}{A_{w'}} \quad (6.2)$$

By choosing

$$A_w = \frac{1}{\epsilon \cdot \pi(w)} \quad \forall w \in \mathcal{W} \quad (6.3)$$

we get a uniform bound on the error probability

$$\Pr\{E_w\} \leq \epsilon \cdot \sum_{w' \neq w} \pi(w') \leq \epsilon \quad (6.4)$$

which also implies

$$P_e \leq \epsilon \quad (6.5)$$

Thus, for an appropriate choice of message-dependent threshold values, the average probability of error for the entire message set is bounded by ϵ . Recall, however, that the effective rate depends on the threshold value and therefore needs to be reexamined here. When different thresholds are used for different messages, the stopping time depends on which message crosses the threshold. We can therefore use Wald's equation (4.9) conditioned on the true message:

$$\mathbb{E}\{T|W = w\} \leq \frac{a_w + C}{C} \quad (6.6)$$

where

$$a_w = \log A_w = -\log \pi(w) - \log \epsilon \quad (6.7)$$

Averaging on the entire message set, we have

$$\begin{aligned} \mathbb{E}\{T\} &= \mathbb{E}\{\mathbb{E}\{T|W\}\} \leq \frac{\mathbb{E}\{a_w\} + C}{C} \\ &= \frac{\mathbb{E}\{-\log \pi(W)\} - \log \epsilon + C}{C} \\ &= \frac{H(W) - \log \epsilon + C}{C} \end{aligned} \quad (6.8)$$

where $H(W)$ is the entropy rate of the source in bits per symbol. Let us now examine (6.8) in a practical setting. Suppose we wish to convey blocks of K source bits with fixed probability of error $\epsilon > 0$. Since every source symbol

contains $\log M$ bits, $K/\log M$ source symbols will be needed. Thus, the rate at which source bits can be conveyed over the channel will be

$$R = \frac{K}{\mathbb{E}\{T\}} \geq \frac{K \cdot C}{\frac{K \cdot H(W)}{\log M} - \log \epsilon + C} \quad (6.9)$$

$$= \frac{C}{\mathcal{H}(W) + \frac{C - \log \epsilon}{K}} \quad (6.10)$$

$$= \frac{C}{\mathcal{H}(W)} \cdot \frac{1}{1 + \frac{C - \log \epsilon}{\mathcal{H}(W) \cdot K}} \quad (6.11)$$

$$= \frac{C}{\mathcal{H}(W)} \cdot \left(1 - O\left(\frac{1}{K}\right)\right) \quad (6.12)$$

where we define $\mathcal{H}(W) = H(W)/\log M$ as the per-bit entropy of the source.

Note that the encoder used here, as well as the codebook, are the same ones defined in Chapter 2 and the only change is in the definition of the decoder. The encoder is uninformed on the statistics of the source or the capacity of the channel, yet the rate approaches the optimum rate achievable by an informed encoder. We note the practical implication of such scheme: the compression algorithms can be implemented and maintained at the decoder, while the encoder remains simple and source-independent.

6.2 Source Coding with Side Information

Suppose now, that the source of information emits independent pairs of messages $(W_1, W_2) \in \mathcal{W}_1 \times \mathcal{W}_2$ according to a probability distribution $\pi_{w_1, w_2}(w_1, w_2)$, which are encoded separately and pass through a noiseless channel. Suppose that R_1 and R_2 are the coding rates of W_1 and W_2 , respectively. By Slepian-Wolf theorem, if W_1 is encoded with rate $R_1 \geq H(W_1)$, then W_2 can be encoded independently with $R_2 = H(W_2|W_1)$. (This rate pair is a corner point in the achievable rate region.) We will now show that using rateless codes, we can approach this rate with some redundancy due to the usage of finite message set. The encoder of W_1 assigns to each message in \mathcal{W}_1 an infinite codeword $\mathbf{c}_{w_1} \in \{0, 1\}^\infty$, $w_1 = 1, \dots, |\mathcal{W}_1|$, and transmits it over the channel. The encoder of W_2 operates similarly to that of W_1 and independently of it, with codewords $\mathbf{d}_{w_2} \in \{0, 1\}^\infty$, $w_2 = 1, \dots, |\mathcal{W}_2|$.

The codewords are assumed to be i.i.d. Bernoulli(1/2) sequences. To reconstruct W_1 , the decoder can use the decision rule (6.1), to obtain an error probability of

$$\Pr\{\hat{W}_1 \neq W_1\} \leq \frac{\epsilon}{2} \quad (6.13)$$

Since binary code is used and the channel is noiseless, we have $C = 1$, so (6.8) implies that the expected transmission time for W_1 satisfies

$$R_1 = \mathbb{E}\{T_1\} \leq H(W) - \log \frac{\epsilon}{2} + 1 \quad (6.14)$$

Note that the coding rate is defined here as the average codeword length for the message set. Therefore, the effective rate equals the expected transmission time, rather than its reciprocal as in channel coding.

Having decoded message W_1 , the decoder uses the following decision rule to reconstruct W_2 :

$$g_n^{(2)}(y^n, w_1) = \begin{cases} w_2, & z_{w_2,1} + \dots + z_{w_2,n} \geq a(w_1, w_2) \\ 0, & \text{if no such } w_2 \text{ exists} \end{cases} \quad (6.15)$$

where

$$z_{w_2,k} = \log \frac{p(y_k | d_{w_2,k})}{p(y_k)}, \quad k = 1, \dots, n \quad (6.16)$$

Similar derivation for the error probability as in Section 6.1 yields

$$\Pr\{\hat{W}_2 \neq w_2 \mid W_1 = w_1, W_2 = w_2\} \leq \sum_{w'_2 \neq w_2} \frac{1}{A(w_1, w_2)} \quad (6.17)$$

We choose

$$A(w_1, w_2) = \frac{1}{\epsilon/2 \cdot \pi_{w_2|w_1}(w_2|w_1)} \quad (6.18)$$

so that

$$\Pr\{\hat{W}_2 \neq w_2 \mid W_1 = w_1, W_2 = w_2\} \leq \epsilon/2 \cdot \sum_{w'_2 \neq w_2} \pi_{w_2|w_1}(w_2|w_1) \leq \frac{\epsilon}{2} \quad (6.19)$$

Therefore,

$$\Pr\{\hat{W}_2 \neq W_2\} \leq \frac{\epsilon}{2} \quad (6.20)$$

Using (6.13), (6.20) and the union bound, we have

$$\Pr\{\hat{W}_1 \neq W_1 \cup \hat{W}_2 \neq W_2\} \leq \epsilon \quad (6.21)$$

Since $a(w_1, w_2) = -\log \epsilon/2 - \log \pi_{w_2|w_1}(w_2|w_1)$, we can use Wald's equation for the stopping time of decoding W_2 to obtain

$$\begin{aligned} R_2 &= \mathbb{E}\{T_2\} = \mathbb{E}\{\mathbb{E}\{T_2|W_1, W_2\}\} \\ &\leq \mathbb{E}\{a(W_1, W_2)\} + 1 \\ &= \mathbb{E}\{-\log \pi_{w_2|w_1}(W_2|W_1)\} - \log \frac{\epsilon}{2} + 1 \\ &= H(W_2|W_1) - \log \frac{\epsilon}{2} + 1 \end{aligned} \quad (6.22)$$

Combining (6.14) and (6.22), we get

$$R_1 + R_2 = H(W_1, W_2) - 2 \log \frac{\epsilon}{2} + 2 \quad (6.23)$$

Similarly to Section 6.1, if we take blocks of K source bits and a fixed error probability $\epsilon > 0$, we obtain

$$R_1 + R_2 = H(W_1, W_2) \cdot \left(1 + O\left(\frac{1}{K}\right)\right) \quad (6.24)$$

6.3 Complete Universality

We now consider the case of joint source-channel coding of an unknown source over an unknown channel, with an unknown amount of side-information at the receiver. Initially, we bring together the results of the previous sections to obtain a communication scheme for a source with unknown statistics over an unknown channel. As a straightforward generalization of the universal source coding scheme in Section 5.1, we use a fusion of the decoders (5.6) and (6.1), i.e.

$$g_n(y^n) = \begin{cases} w, & p_U(\mathbf{c}_w|y^n) \geq A_w \cdot q(\mathbf{c}_w) \\ 0, & \text{if no such } w \text{ exists} \end{cases} \quad (6.25)$$

where

$$A_w = \frac{1}{\epsilon \cdot \pi(w)} \quad (6.26)$$

Similar derivation to those done at Sections 5.1 and 6.1 yields the following rate for an uncompressed source $W \in \{1, \dots, M\}$ over an unknown channel with capacity C :

$$R = \frac{C \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{\log M \ln 2}\right)}{\mathcal{H}(W) + \frac{C + \beta - \log \epsilon + \frac{|\mathcal{X}||\mathcal{Y}|}{2} (\log \log M - \log C - \frac{1}{\ln 2})}{\log M}} \quad (6.27)$$

where $\mathcal{H}(W)$ is defined in Section 6.1. We note that while the encoder can be ignorant of the source statistic, the decoder needs to know $\pi(w)$, $w \in \mathcal{W}$.

We now go one step further and assume that the decoder has no knowledge of the statistics of the source or the channel. Suppose that the source S generates sequences of L symbols from an alphabet \mathcal{S} , drawn i.i.d. according to set of $|\mathcal{S}|$ unknown probabilities γ . Each sequence is encoded as one message, hence $M = |\mathcal{S}|^L$. Instead of using the set of thresholds (6.26), which depends on the unknown probabilities, we use a universal probability measure [10]

$$\hat{\pi}(s^L) = \int u(\gamma) \pi_\gamma(s^L) \quad (6.28)$$

so that

$$a_w = \log A_w = -\log \epsilon - \log \hat{\pi}(s^L) \quad (6.29)$$

If the weight function $u(\cdot)$ is chosen to be Jeffreys prior, we get (see [10, Eq.17])

$$\mathbb{E}\{a_w\} = -\log \epsilon + H(W) + \frac{|\mathcal{S}| - 1}{2} \log \frac{L}{2\pi e} + O(1) \quad (6.30)$$

Hence, similarly to (6.27) we can achieve the following rate

$$R = \frac{C \left(1 - \frac{|\mathcal{X}||\mathcal{Y}|/2}{\log M \ln 2}\right)}{\hat{\mathcal{H}}(W) + \frac{C + \beta - \log \epsilon + \frac{|\mathcal{X}||\mathcal{Y}|}{2} (\log \log M - \log C - \frac{1}{\ln 2})}{\log M}} \quad (6.31)$$

where

$$\hat{\mathcal{H}}(W) = \mathcal{H}(W) + \frac{|\mathcal{S}| - 1}{2} \frac{\log L}{\log M} + O\left(\frac{1}{\log M}\right) \quad (6.32)$$

Recall that $L = \log_{|\mathcal{S}|} M$, so

$$\hat{\mathcal{H}}(W) = \mathcal{H}(W) + \frac{|\mathcal{S}| - 1}{2} \frac{\log \log M}{\log M} + O\left(\frac{1}{\log M}\right) \quad (6.33)$$

By plugging (6.33) into (6.31) we get

$$R = \frac{C}{\mathcal{H}(W)} \cdot \left(1 - O\left(\frac{\log K}{K}\right)\right) + O\left(\frac{1}{K}\right) \quad (6.34)$$

where $K = \log M$ is the number of encoded bits. Comparing (6.34) to (6.12), we see that the leading term is unchanged and equals the optimal rate achievable by separated source-channel coding. However, the lack of information affects the rate of convergence, which is now dominated by a $O\left(\frac{\log K}{K}\right)$ term, as opposed to $O\left(\frac{1}{K}\right)$ for an informed decoder.

The implications of the latter result are far-reaching. We have shown that even if the statistics of both the channel and the source are unknown to the decoder, rateless coding not only achieves the best source-channel coding rate as $M \rightarrow \infty$, but it also has the same asymptotics of a rateless scheme with an informed decoder. This observation has been made in [1, Ch.4] for infinitely large message sets. The results obtained here coincide with those of [1], and also quantify the redundancy caused by the lack of information on the source and the channel, and by the use of finite blocks.

Unknown Side Information at the Decoder

Similarly to Section 6.2, if the source contains side information V that is known non-causally at the decoder, we can further improve the communication rate. Combining the technique from Section 6.2 with the derivation above, we obtain the following rate for universal joint source-channel coding with side information at the decoder:

$$R = \frac{C}{\mathcal{H}(W|V)} \cdot \left(1 - O\left(\frac{\log K}{K}\right)\right) + O\left(\frac{1}{K}\right) \quad (6.35)$$

where $\mathcal{H}(W|V)$ is the conditional entropy of the source W given the side information V , normalized by $\log M$. Since $\mathcal{H}(W|V) \leq \mathcal{H}(W)$, the side information improves the rate, even if the encoder is uninformed on the amount (or the existence) of the side information.

Chapter 7

Summary

In this study we developed and analyzed several communication schemes that are all based on the concept of *rateless codes*. In rateless codes, each codeword has an infinite length and the decoding length is dynamically determined by the confidence level of the decoder. Throughout this study, we allowed the coding schemes to have a fixed error probability, while aiming to achieve shortest mean transmission time, or equivalently, the highest rate. This approach is different than the prevalent one, in which the communication rate is held fixed and the codebook is enlarged indefinitely so that the error probability vanishes. We demonstrated how rateless codes, combined with sequential decoding, can be used in basic communication scenarios such as communication over a DMC, but can also be used to solve more complex problems, such as communication over an unknown channel. The decoding methods introduced here enabled us to obtain results for finite message set, while previous studies were restricted to asymptotic results.

We began by describing rateless codes and surveyed some previous results related to such coding schemes. Then, we introduced the sequential decoder that uses a known channel law. Using Wald's theory and the notion of stopping time, we obtained an upper bound for the mean transmission time for a fixed error probability, and the resulting effective rate is shown to approach to the capacity of the channel as the size of the message set, M , grows. We also obtained an upper bound for the rate for a fixed error probability. The upper bound is not tight for small M , but it converges to the achievable rate as $M \rightarrow \infty$. We conjecture that a stronger converse can be found, which will be tighter also in the non-asymptotic

realm. Although we developed the above-mentioned scheme for a DMC, we also demonstrated that it is applicable in a memoryless Gaussian channel.

For the case of an unknown channel we introduced a novel decoding metric. Unlike previous studies, the universal decoding metric is not based on empirical mutual information, but on a mixture probability assignment. For an appropriate choice of mixture, we were able to bound the difference between the universal metric and the one used by an informed decoder. Thus, we used the results obtained for an informed decoder to upper bound the mean transmission time in the universal case.

We then applied rateless coding to more advanced scenarios. We showed how with only a minor change in the sequential decoder, we can easily use rateless codes as a joint source-channel coding scheme. We also used rateless coding for source coding with side information, obtaining the optimum Slepian-Wolf rate for this setting. Finally, we combined the techniques for universal channel coding, joint source-channel coding and source coding with side information and demonstrated that even without any information on the source, the channel or the amount (or even the existence) of side information—reliable communication is feasible, and the rate can be analyzed even for a finite message set.

Bibliography

- [1] N. Shulman, “Communication over an unknown channel via common broadcasting,” Ph.D. dissertation, Tel Aviv University, 2003.
- [2] T. Cover and J. M. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.
- [3] A. Wald, *Sequential Analysis*. New York: Wiley, 1947.
- [4] I. Csiszár and J. Körner, *Information Theory*. New York: Academic Press, 1981.
- [5] Y. Polyanskiy, H. Poor, and S. Verdú, “Feedback in the non-asymptotic regime,” *IEEE Trans. Information Theory*, vol. 57, no. 8, pp. 4903–4925, Aug. 2011.
- [6] C. E. Shannon, “The zero error capacity of a noisy channel,” *IRE Trans. Information Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.
- [7] M. V. Burnashev, “Data transmission over a discrete channel with feedback. random transmission time,” *Problemy Peredachi Informatsii*, vol. 12, no. 4, pp. 10–30, Jul. 1976.
- [8] A. Tchamkerten and I. E. Telatar, “Variable length coding over an unknown channel,” *IEEE Trans. Information Theory*, vol. 52, no. 5, pp. 2126–2145, May 2006.
- [9] Q. Xie and A. R. Barron, “Asymptotic minimax regret for data compression, gambling and prediction,” *IEEE Trans. Information Theory*, vol. 46, no. 2, pp. 431–445, Mar. 2000.

- [10] M. Feder and N. Merhav, “Universal prediction,” *IEEE Trans. Information Theory*, vol. 44, no. 6, pp. 2126–2145, Oct. 1998.
- [11] P. Berlin, B. Nakiboglu, B. Rimoldi, and E. Telatar, “A simple converse to Burnashev’s reliability function,” *IEEE Trans. Information Theory*, vol. 55, no. 7, pp. 3074–3080, Jul. 2009.
- [12] D. Williams, *Probability with Martingales*. Cambridge, U.K.: Cambridge University Press, 1991.
- [13] S. Verdu and S. Shamai (Shitz), “Variable-rate channel capacity,” *IEEE Trans. Information Theory*, vol. 56, no. 6, pp. 2651–2667, Jun. 2010.
- [14] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.